

特開平8-329011

(43)公開日 平成8年(1996)12月13日

| (51) Int. Cl. <sup>6</sup> | 識別記号 | 庁内整理番号  | F I        | 技術表示箇所 |   |
|----------------------------|------|---------|------------|--------|---|
| G06F 15/00                 | 330  | 9364-5L | G06F 15/00 | 330    | Z |
| 12/00                      | 537  | 7623-5B | 12/00      | 537    | H |
| 17/60                      |      | 7259-5J | G09C 1/00  |        |   |
| G09C 1/00                  |      |         | G06F 15/21 |        | Z |
| H04L 9/06                  |      |         | H04L 9/02  |        | Z |

審査請求 未請求 請求項の数2 OL (全10頁) 最終頁に続く

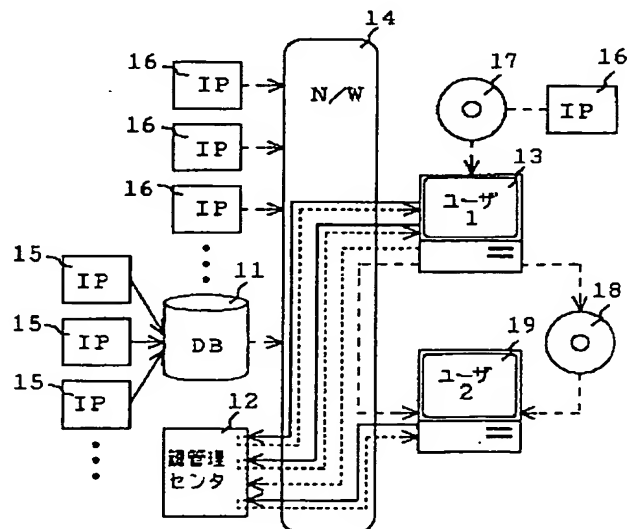
|          |                |         |   |
|----------|----------------|---------|---|
| (21)出願番号 | 特願平7-136808    | (71)出願人 | 000005979<br>三菱商事株式会社<br>東京都千代田区丸の内2丁目6番3号      |
| (22)出願日  | 平成7年(1995)6月2日 | (71)出願人 | 000006013<br>三菱電機株式会社<br>東京都千代田区丸の内2丁目2番3号      |
|          |                | (72)発明者 | 斎藤 誠<br>東京都千代田区丸の内2丁目6番3号 三<br>菱商事株式会社内         |
|          |                | (72)発明者 | 岡崎 正一<br>神奈川県鎌倉市上町屋325番地 三菱電機<br>株式会社情報システム製作所内 |
|          |                | (74)代理人 | 弁理士 南條 眞一郎                                      |

(54) 【発明の名称】 データ著作権管理システム

(57) 【要約】

【目的】 1次ユーザが入手したデータを加工し、加工されたデータを2次利用者へ供給するデータ著作権管理システムを提供する。

【構成】 データベース、鍵管理センタを備え、１次著作権ラベル、第１暗号鍵を含む１次利用鍵、２次利用鍵、第３暗号鍵、著作権管理プログラムが用いられる。１次ユーザは第１暗号鍵を用いて暗号化されて供給された１次著作権データを鍵管理センタから入手した１次利用鍵で平文化し利用するが、保存する場合には１次利用鍵を用いて再暗号化される。１次ユーザは鍵管理センタから１次著作権データ加工用の２次利用鍵を入手して１次著作権データの加工を行い、加工途中のデータは２次利用鍵で暗号化されて保存される。１次ユーザは加工が終了すると２次著作兼用の第３暗号鍵を鍵管理センタから受け取り、加工済みデータを第３暗号鍵で暗号化し、２次ユーザに配布する。２次ユーザは鍵管理センタから第３暗号鍵を入手し、加工データを利用する。



## 【特許請求の範囲】

【請求項 1】 データベースおよび鍵管理センタを備え、データ著作物を入手した 1 次ユーザが入手した 1 次著作権データを加工し、加工によって得られた 2 次著作権データを 2 次利用者へ供給する場合に著作権を管理するデータ著作権管理システムであって：前記 1 次著作権データが 1 次利用鍵を用いて暗号化されて前記 1 次ユーザに供給され；前記 1 次著作権データの利用を希望する前記 1 次ユーザからの前記 1 次利用鍵の配布要求に対し、前記鍵管理センタが前記 1 次利用鍵を前記 1 次ユーザに配布し；前記 1 次ユーザは配布された前記 1 次利用鍵を用いて前記 1 次著作権データを平文化して 1 次利用を行い；前記 1 次著作権データの加工を希望する前記 1 次ユーザは前記鍵管理センタから前記 1 次著作権データを加工するための 2 次利用鍵の配布を受け、配布された前記第 2 利用鍵を用いて前記 1 次著作権データの加工を行い、加工中の著作権データは前記第 2 利用鍵を用いて暗号化されて保存され；加工が終了した前記 1 次ユーザは前記鍵管理センタから加工済みデータを配布するための第 3 暗号鍵の配布を受け、前記加工済みデータを前記第 3 暗号鍵を用いて暗号化して 2 次ユーザに供給し；前記 2 次著作権データの利用を希望する前記 2 次ユーザは前記鍵管理センタから前記第 3 暗号鍵の配布を受け、配布された前記第 3 暗号鍵を用いて前記 2 次著作権データを平文化して利用する；データ著作権管理システム。

【請求項 2】 前記 1 次ユーザによる前記 1 次著作権データの加工が、前記 1 次著作権データの複写物に対して行われる請求項 1 記載のデータ著作権管理システム。

## 【発明の詳細な説明】

## 【 0 0 0 1 】

【産業上の利用分野】 本発明はディジタルデータの利用、すなわち表示、保存、複写、加工、転送において著作権を管理するシステムに係るものである。

## 【 0 0 0 2 】

【従来の技術】 情報化時代と言われる今日、通常の地上波放送(terrestrial broadcasting)の他に放送衛星(Broadcasting Satellite: BS)、通信衛星(Communication Satellite: CS)と呼ばれる衛星放送、同軸ケーブルあるいは光ケーブルを利用した CATV (Cable Television) と呼ばれる有線 TV 放送が普及しつつある。

【 0 0 0 3 】 同時に数 1 0 チャンネルを配信することができる衛星放送あるいは CATV 放送においては、包括的な契約によって視聴することができるスクランブルがかけられていない一般的なチャンネルの他に、包括的な契約によっては視聴することができないスクランブルされた映画・スポーツ・音楽等専門的なチャンネルが設けられている。これらのチャンネルを視聴するためにはスクランブルを解除するするために契約を行う必要があるが、この契約期間は通常 1 か月程度の単位で行われるため、随時の契約によって視聴することができない。

【 0 0 0 4 】 この問題に対応するために、本発明者らは特開平 6 - 4 6 4 1 9 号及び特開平 6 - 1 4 1 0 0 4 号で公衆電信電話回線を通じて課金センタから視聴許可鍵を入手するとともに課金が行われ、視聴許可鍵を用いて番組毎に異なるスクランブルパターンで行われたスクランブルを解除して番組を視聴するシステムを、特開平 6 - 1 3 2 9 1 6 号でそのための装置を提案した。これらのシステム及び装置において、スクランブルされた番組の視聴を希望する者は通信装置を使用し通信回線を経由して課金センタに視聴申し込みを行い、課金センタはこの視聴申し込みに対して通信装置に許可鍵を送信するとともに課金処理を行い料金を徴収する。通信装置で許可鍵を受信した視聴希望者は通信装置と受信装置を接続する直接的な手段あるいはフレキシブルディスク等の間接的な手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって番組のスクランブルを解除する。

【 0 0 0 5 】 特開平 6 - 1 3 2 9 1 6 号にはこれらのシステム及び装置の応用として、各々異なるスクランブルパターンでスクランブルされた複数のデータが記録されたテープあるいはディスクを販売あるいは貸与し、IC カード等により許可鍵を供給して特定のデータを利用するシステム及び装置も記載されている。

【 0 0 0 6 】 また、情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータを LAN (Local Area Network) と呼ばれる局所的ネットワーク、WAN (Wide Area Network) と呼ばれる国単位のネットワークさらにはこれらを国際的に拡大したインターネット (InterNet) と呼ばれるネットワークによってコンピュータ通信ネットワークシステムを構成し、相互に利用するデータベースシステムが普及しつつある。

【 0 0 0 7 】 一方、デジタル化すると情報量が膨大になるためデジタル化することができなかったテレビジョン動画信号を圧縮することにより情報量を減少させ、実用的なデジタル化を可能にする技術が開発され、これまでにテレビジョン会議用の H. 2 6 1 規格、静止画像用の J P E G (Joint Photographic image coding Experts Group) 規格、画像蓄積用の M P E G 1 (Moving Picture image coding Experts Group 1) 規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応する M P E G 2 規格が作成された。

【 0 0 0 8 】 これらの画像圧縮技術を利用したデジタル化技術はテレビジョン放送あるいはビデオ画像記録用に用いられるだけではなく、コンピュータでこれまで扱うことができなかったテレビジョン動画データが扱うことができるようになり、コンピュータが扱う各種のデータとデジタル化されたテレビジョン動画データを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。このマルチメディアシステムもデータ

通信に組み入れられ、データベース上のデータの一つとして利用される。

【0009】このようにしてデータベースの利用範囲が拡大する中で、データベース上のデータ利用に対する課金をどのようにして行うかということ及びデータの直接的な利用以外の複写あるいは転送等によって発生する著作権の問題及びデータの加工によって発生する2次的著作権の問題をどのようにして処理するかということが重要になる。課金及び著作権の処理を確実に行うには、正規の利用者でなければデータの利用が不可能であるようにする必要があり、データを暗号化しておくことがそのための最良の手段である。

【0010】これらのテレビジョンシステムあるいはデータベースシステムにおいて、データを暗号化し、暗号化されたデータを復号して利用するためには暗号鍵が必要であり、データ利用者に対して暗号鍵を渡さなければならないが、この作業は安全性及び確実性が要求されるため非常に煩雑である。

【0011】本発明はその構成において暗号技術が重要な役割を果たすが、初めに一般的な暗号技術について説明する。暗号技術においては、平文Mを暗号鍵Kを用いて暗号化し暗号文Cを得る暗号化 (Encryption) を  $C = E(K, M)$  と表現し、暗号文Cを暗号鍵Kを用いて復号化し平文Mを得る復号化 (Decryption) を  $M = D(K, C)$  と表現する。

【0012】さらに、本発明者らは特願平6-64889号においてデータ著作権管理システムの具体的な構成を提案した。このシステムでは、デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータの表示 (音声化を含む)、保存、複写、加工、転送における著作権の管理を行うために、利用申し込み者に対して暗号化されたデータの利用を許可する鍵の他に、必要に応じて著作権を管理するためのプログラム、著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を送信する。著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムは申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0013】また、データは暗号化されて供給され、許可鍵を用いて復号化され利用されるが、装置内への保存、装置外の媒体への複写、装置外への転送が行われる場合には暗号化される。また、表示・利用、保存、複写、加工、転送等の利用形態各々に対して許可鍵が用意される。

【0014】

【発明の概要】本発明のシステムはデータベース、鍵管

理センタ、1次ユーザ、2次ユーザおよびこれらを相互に接続するネットワークシステムから構成され、1次著作権ラベル、第1暗号鍵を含む1次利用鍵、第2暗号鍵を含む2次利用鍵、2次著作権ラベル、第3暗号鍵、著作権管理プログラムが用いられる。平文1次著作権データは1次暗号鍵を用いて暗号化された状態で、1次ユーザに供給され、暗号1次著作権データの利用を希望する1次ユーザは、鍵管理センタにネットワークシステムを経由して1次利用鍵の配布を要求し、1次ユーザからの1次利用鍵の配布要求を受けた鍵管理センタは1次利用鍵を1次ユーザに配布し、このときに課金を行う。

【0015】1次ユーザは配布された1次利用鍵に含まれる第1暗号鍵を用いて暗号化1次著作権データを平文化し利用するが、平文1次著作権データを1次ユーザの装置内へ保存する場合には1次利用鍵を用いて再暗号化される。1次著作権データの加工を希望する1次ユーザが平文1次著作権データの加工を行うための2次利用鍵の配布をネットワークシステムを経由して鍵管理センタに要求すると、鍵管理センタは2次利用鍵を1次ユーザに配布する。2次利用鍵を受け取った1次ユーザは1次著作権データの複写を作成し、複製された1次著作権データの加工を行い、加工途中の平文2次著作権データを2次利用鍵に含まれた第2暗号鍵により暗号化し、最終加工データは第3暗号鍵を用いて暗号化して1次ユーザの装置内に保存する。1次ユーザは2次著作権データのデータ加工についての2次著作権を行使するために鍵管理センタに第3暗号鍵を登録し、暗号2次著作権データを第3暗号鍵を用いて暗号化して外部記憶媒体への複写あるいはネットワークシステムを介して転送することにより2次ユーザへ供給する。

【0016】暗号2次著作権データの利用を希望する2次ユーザは、鍵管理センタに第3暗号鍵の配布を要求し、第3暗号鍵の配布要求を受けた鍵管理センタは、第3暗号鍵をネットワークシステムを経由して2次ユーザに配布する。2次暗号鍵を受け取った2次ユーザは2次暗号鍵を用いて暗号2次著作権データを復号し、利用する。

【0017】

【実施例】以下、図面を用いて本発明の実施例を説明する。初めに、本発明が対象とするデータ著作権管理システムの構成を図1を用いて説明する。図1に示されたシステムはデータベース1、鍵管理センタ2、ユーザ3、3、3・・・およびこれらを相互に接続するネットワークシステム4から構成されている。また、データベース1には情報提供者 (Information Provider: IP) 5、5、5・・・からデータが供給されるが、場合によってはデータベース1を経由することなく情報提供者6、6、6・・・からネットワークシステム4を経由して直接にユーザ3に対してデータが供給されることがある。なお、本発明において利用するデータはプログラムとデ

ータが組み合わされてオブジェクトである。ユーザ3は単なる利用者ではなく入手した複数の著作権データを組み合わせたり、修正したりすることにより新しい著作物（2次著作物）を提供する情報提供者5あるいは6となる。

【0018】このように構成される本発明のデータ著作権管理システムにおいて、各情報提供者5、6から提供される著作権データは著作権を保護するために暗号化されている。したがって、暗号著作権データを入手したユーザ3が利用するには暗号著作権データを復号する必要がある。そのため、このシステムにおいて暗号鍵はすべて鍵管理センタ2に預けられ、鍵管理センタ2が管理している。また、各情報提供者5、6が採用する暗号方式は自由であるが後で述べる2次利用以降で使用される暗号方式は鍵センタが採用する方式に限られる。

【0019】データベースからのデータ利用は一般的にパーソナルコンピュータを用いて行われるが、そこで用いられるOSとしてはセキュリティ対応処理を組み込んでいるものを使用する必要がある。また、暗号鍵等の管理を行うために著作権管理プログラムが使用されるが、この著作権管理プログラムおよび鍵管理センタ2から受け取った暗号鍵を保管しておく必要があるため、メモリあるいはHDD上にソフトウェア的に実現されあるいは専用のボード、PCカード等でハードウェアとして実現される「キーカード」がこれらの保管場所として用意される。

【0020】鍵管理センタ2は、実際に利用されているか単に登録されているのみで利用されていないかを問わず、データ著作物の著作権の保護と著作権の利用に対する課金を行うために鍵を保管し、保管されている鍵と著作権ラベルの対応付けを行うことにより鍵の管理を行う。

【0021】図2に示されたのは、情報提供者からデータ著作物を入手した1次ユーザが、入手したデータを加工し、加工されたデータを2次利用者へ供給する本発明のデータ著作権処理システム実施例の概要構成である。このシステムにおいては平文1次著作権データD1、暗号1次著作権データ（Encrypted Data）ED1i、平文2次著作権データD2、暗号2次著作権データED2j、平文1次著作権ラベル（Label）LC1、第1暗号鍵（Key）K1iを含む1次利用鍵K1、2次利用鍵K2、第3暗号鍵K3j、平文著作権管理プログラムPCが用いられる。

【0022】このシステムはデータベース11、鍵管理センタ12、1次ユーザ13、2次ユーザ19およびこれらを相互に接続するネットワークシステム14から構成される。また、データベース11には情報提供者15、15、15・・・からデータが供給されるが、場合によってはデータベース11を経由することなく情報提供者16、16、16・・・からネットワークシステム14を経由してあるいは情報提供者16からCDROM

等の情報記録媒体17を介して直接にユーザ13に対してデータが供給されることがある。なお、この図において実線で示されたのは平文データの経路、破線で示されたのは暗号データの経路、点線で示されたのは鍵の経路である。

【0023】このシステムにおいて、平文1次著作権データD1iは第1暗号鍵K1iを用いて暗号化された状態で暗号1次著作権データED1iの形で、  
 $ED1i = E(K1i, D1i)$

情報提供者15からデータベース11を介してネットワークシステム14を経由して、情報提供者16からネットワークシステム14を経由してあるいはCDROM等の情報記録媒体17を介して1次ユーザ13に供給される。供給された暗号1次著作権データED1iの利用を希望する1次ユーザ13は、鍵管理センタ12にネットワークシステム14を経由して1次著作権ラベルLC1を提示して1次利用鍵K1の配布を要求する。

【0024】1次ユーザ13からの1次利用鍵K1の配布要求を受けた鍵管理センタ12は提示された1次著作権ラベルLC1により1次利用鍵K1を探し出し、1次利用鍵K1をネットワークシステム14を経由して1次ユーザ13に配布し、このときに課金を行う。1次ユーザ13は配布された1次利用鍵K1に含まれる第1暗号鍵K1iを用いて暗号化1次著作権データED1iを平文化し、  
 $D1i = D(K1i, ED1i)$   
 利用する。

【0025】平文1次著作権データD1iを1次ユーザ13の装置内へ保存する場合には第1暗号鍵K1iを用いて再暗号化し、  
 $ED1i = E(K1i, D1i)$   
 暗号化されたデータED1iが保存される。再暗号化されたデータED1iを再利用する場合には第1暗号鍵K1iを用いて再平文化および再暗号化が行われる。

【0026】平文1次著作権データD1iの加工を希望する1次ユーザ13は平文1次著作権データD1iの加工を行うための2次利用鍵K2の配布をネットワークシステム14を経由して鍵管理センタ12に要求する。

【0027】2次利用鍵K2の配布要求を受けた鍵管理センタ12は、2次利用鍵K2をネットワークシステム14を経由して1次ユーザ13に配布する。2次利用鍵K2を受け取った1次ユーザ13は許可鍵の内容に従って平文1次著作権データD1iの加工を行い、平文2次著作権データD2jをユーザ13の装置内に保存する場合には、第2暗号鍵K2によって暗号化される。  
 $ED2j = E(K2, D2j)$

加工が最終的に終了すると、1次ユーザ13は2次著作権データのデータ加工についての2次著作権を行使するために、第3暗号鍵K3jを生成し生成された第3暗号鍵

K3jを鍵管理センタ12に登録する。なお、第3暗号鍵K3jは1次ユーザ13ではなく鍵管理センタ12が作成し、1次ユーザ13からの要求により配布するようにしてもよい。

【0028】1次ユーザ13が平文暗号2次著作権データED2jを外部記憶媒体18への複写あるいはネットワークシステム14を介して転送する場合には、平文2次著作権データED2jを第3暗号鍵で暗号化し、  
ED3j=E(K3j, D2j)  
2次ユーザ19へ供給する。

【0029】供給された暗号2次著作権データED3jの利用を希望する2次ユーザ19は、鍵管理センタ12にネットワークシステム14を経由して第3暗号鍵K3jの配布を要求する。2次ユーザ19からの第3暗号鍵K3jの配布要求を受けた鍵管理センタ12は第3暗号鍵K3jをネットワークシステム14を経由して2次ユーザ19に配布する。第3暗号鍵K3jを受け取った2次ユーザ19は、第3暗号鍵K3jを用いて暗号2次著作権データED2jを復号し、  
D2j=D(K3j, ED2j)  
利用する。その場合も、暗号化データED2jを再度利用する場合には第3暗号鍵K3jを用いて復号化および暗号化が行われる。

【0030】1次著作権データの入手、1次著作権データの1次利用、1次著作権データの加工、加工された2次著作権データの供給および2次著作権データの利用について詳細に説明する。このシステムにおいて、複数の1次著作権データD1iは1次暗号鍵K1iを用いて暗号化された状態で  
ED1i=E(K1i, D1i)

平文1次著作権ラベルLC1とともに、情報提供者11から直接にあるいはデータベースを介して、1次ユーザ13に供給される。

【0031】著作権管理プログラムPCはユーザによる著作権データの使用を管理するものであり、具体的には与えられた暗号鍵を用いての著作権データの復号化及び再暗号化および利用鍵の内容に従う著作権データの利用制限を行う。このシステムにおいて提供される暗号データED1jには暗号鍵入手等に利用するための平文の1次著作権ラベルLC1が付けられており、すなわち、暗号1次著作権データED1は平文1次著作権ラベルLC1と暗号1次著作権データED1iから構成されている。平文1次著作権ラベルLC1にはデータのタイトル名、使用しているアプリケーション・プログラム名、1次著作権者が記入されている。供給された暗号1次著作権データED1iの利用を希望する1次ユーザ13は、鍵管理センタ12にネットワークシステム14を経由して平文1次著作権ラベルLC1を提示して1次利用鍵K1の配布を要求する。

【0032】提示された1次著作権ラベルLC1により、

配布すべき1次利用鍵が鍵K1であることを確認した鍵管理センタ12は確認された1次利用鍵K1をネットワークシステム14を経由して1次ユーザ13に配布する。配布された1次利用鍵K1を受信した時点で1次ユーザ13の装置は著作権管理モードになり、1次ユーザ13は1次著作権データの利用が可能になる。なお、第1暗号鍵K1iは1次利用鍵K1に含まれているため、1次ユーザ13から第1暗号鍵K1iは認識されない。一方、鍵管理センタ12は課金処理を行うとともに著作権データの使用状況および1次ユーザ13のデータベース利用状況を把握する。

【0033】図3に示されたのは、本発明において著作権管理プログラムPCが行う1次利用の制限を説明する概念図である。先願である特願平6-64889号に記載された発明と同様に、本願発明のデータ著作権管理システムにおける入手したデータの1次利用は通常の利用形態すなわちデータの直接的な利用およびその利用結果の印刷を含む出力に限定され、外部記憶媒体への複写あるいはネットワークシステムを経由しての転送及び加工、さらに原則としてデータの装置内部での保存を行うことはできない。ただし、データが暗号化されている場合には保存は可能である。なお、使用中のアプリケーション・プログラムにより著作権データ以外のデータDを表示・印刷・保存・複写・加工・転送することが可能なことはいうまでもない。

【0034】この図において21は1次ユーザの装置20内に内蔵された不揮発性半導体メモリあるいはハード・ディスク・ドライブ等の記憶装置、22は出力用の表示装置、23は出力用の印刷装置、D1は1次著作権データ、Dは一般データ、24はフレキシブルディスクあるいはCDROMによる複写、ネットワークシステムによる転送でデータを供給される2次ユーザである。なお、この図において実線で示されたのは許される処理経路、点線で示されたのは許されない処理経路である。

【0035】1次ユーザ13が外部の情報提供者15あるいは16から、直接にあるいはデータベース11を介して入手した暗号1次著作権データED1iはともに供給される平文1次著作権ラベルLC1と組み合わせられて1次ユーザ装置20の記憶装置21に格納される。記憶装置21に格納されている暗号1次著作権データED1iの1次利用を希望する1次ユーザ13は著作権管理プログラムPCにより暗号1次著作権データED1iの概要説明および暗号1次著作権データED1iが使用しているアプリケーション・プログラムの情報等が表示された平文1次著作権ラベルLC1を参照し、暗号著作権1次データED1i作成に使用されているアプリケーション・プログラムの有無等この暗号著作権1次データED1iの使用環境を確認する。

【0036】その結果、暗号著作権1次データED1iの利用が可能であると判断され、1次利用者13がこの暗

10

20

30

40

50

号 1 次著作権データ E Dli を使用することを著作権管理プログラム PC に入力すると、著作権管理プログラム PC は暗号 1 次著作権データ E Dli が使用しているアプリケーション・プログラムを起動し、暗号 1 次著作権データ E Dli を記憶装置 2 1 から装置内のメモリに読み込む。その一方、平文 1 次著作権ラベル L C1 が鍵管理センタ 1 2 に送られ、その結果、前に述べた処理フローにしたがい 1 次利用鍵 K1 が供給されると、1 次利用鍵 K1 に含まれている 1 次暗号鍵 K1i を用いて暗号 1 次著作権データ E Dli が平文 1 次著作権データ Dli に平文化され、

$Dli = D(K1i, E Dli)$   
 起動されたアプリケーション・プログラムによって使用することが可能となる。

【0037】装置 2 0 のメモリ上の平文 1 次著作権データ Dli を記憶装置 2 1 に保存する場合には第 1 暗号鍵 K1i を用いて暗号化して、  
 $E Dli = E(K1i, Dli)$

保存が行われる。この保存には、データ保全のための一時的ファイル (Temporaly File) の作成・保存も含まれる。再暗号化されたデータ E Dli を再利用する場合には第 1 暗号鍵 K1i を用いて再復号化および再暗号化が行われる。なお、平文 1 次著作権データ Dli あるいは暗号 1 次著作権データ E Dli の表示・印刷、保存あるいは加工以外の利用形態すなわち外部記憶媒体への複写および他の装置への転送は著作権管理プログラム PC により禁止される。

【0038】前に述べたように本発明のデータ著作権管理システムにおいて、入手した著作権データは通常の利用形態すなわちデータを表示装置 2 2 に表示することによって直接的な利用を行うことおよびその利用結果をプリンタ 2 3 で出力することに限定され、外部記憶媒体への複写あるいはネットワークシステムを経由しての 2 次ユーザ 2 4 への転送および加工を行うことはできない。したがって、1 次著作権データ Dli の 1 部を切り出して他のデータ D に張り付けること (Cut & Paste) および他のデータ D の 1 部を切り出して 1 次著作権データ Dli に張り付けることは著作権管理プログラムによって禁止される。また、1 次著作権データ Dli は第 1 暗号鍵 K1i を用いて暗号化された状態ならば例外的に記憶装置 2 1 に保存することができるが、何らかの加工が行われた場合に保存は禁止される。

【0039】本発明のデータ著作権管理システムにおいて、1 次著作権データ D1 と一般データ D との区別および著作権データが加工されたか否かは、著作権管理プログラム PC が判別する。コンピュータファイルはファイル本体とそのファイルの属性を記述した管理テーブルから構成されている。したがって、この管理テーブルを調べることによりそのファイルが著作権データであるか否かが判別される。また、この管理テーブルにはファイルサイズ、作成日付が記入されており、これらを調べるこ

とによりファイルの加工が行われたか否かが判別される。

【0040】記憶装置 2 1 に保存されているときに 1 次著作権データ Dli は暗号化されて 1 次著作権ラベル L C1 と結合されているが、メモリ上に読み込まれたときには著作権管理プログラムにより 1 次著作権データ Dli と 1 次著作権ラベル L C1 は分離され、分離された著作権ラベル L C1 は著作権管理プログラム PC により管理される。著作権管理プログラム PC は 1 次著作権データ Dli がどのアプリケーション・プログラムによって使用されているかを監視し、1 次著作権データ Dli の一般データ D への切り出し／張り付けおよび一般データ D の 1 次著作権データ Dli への切り出し／張り付けが行われることを禁止する。

【0041】図 4 に示されたのは、本発明において著作権管理プログラム PC が行うデータ加工利用の制限を説明する概念図である。1 次利用の結果、平文 1 次著作権データ Dli の加工を行うことが適切であると判断されたとき、1 次ユーザ 1 3 は平文 1 次著作権データ Dli の加工を行うことをネットワークシステム 1 4 を経由して鍵管理センタ 1 2 に対して通知する。

【0042】平文 1 次著作権データ Dli の利用を希望する 1 次ユーザ 1 3 は平文 1 次著作権データ Dli の加工を行うための 2 次利用鍵 K2 の配布をネットワークシステム 1 4 を経由して鍵管理センタ 1 2 に要求する。2 次利用鍵 K2 の配布要求を受けた鍵管理センタ 1 2 は 2 次利用鍵 K2 をネットワークシステム 1 4 を経由して 1 次ユーザ 1 3 に配布する。このことにより 1 次ユーザ 1 3 の装置 2 0 は加工モードになり、1 次ユーザ 1 3 は 1 次著作権データの加工が可能になる。

【0043】1 次ユーザ 1 3 は暗号 1 次著作権データ E Dli を第 1 暗号鍵 K1i で平文 1 次著作権データ Dli に平文化した上で表示装置 2 3 に表示してデータの加工を行うが、初めに 1 次著作権データの著作権を保護するために加工用平文 1 次著作権データ Dli の複写が行われ、この複写によって得られた加工用平文 1 次著作権データ Dli' に対して加工が行われる。この加工用平文 1 次著作権データ Dli' あるいはこの加工途中の平文 1 次著作権データ Dli'' をユーザ 1 3 の装置内に保存する場合には 2 次利用鍵 K2 により暗号化されて、

$E Dli' = E(K2, Dli')$

または  $E Dli'' = E(K2, Dli'')$

保存が行われる。暗号 1 次著作権データ E Dli は加工されることなく記憶装置 2 1 内に保存されており、その管理テーブルと加工された加工用平文 1 次著作権データ Dli' あるいは Dli'' のファイルサイズ、作成日付を調べることによりそのファイルが加工されたファイルであるか否かが判別される。

【0044】データの加工が終了するとそのデータは新規な複数の平文 2 次著作権データ D2j となり、これらの

10

20

30

40

50



データD2jについて新たに2次著作権が発生する。この2次著作権を保護するために平文1次著作権D1iを加工した1次ユーザ13は鍵管理センタ12に対して第3暗号鍵K3jの配布を要求し、第3暗号鍵K3jの配布要求を受けた鍵管理センタ12は、第3暗号鍵k3jをネットワークシステム14を経由して1次ユーザ13に配布する。第3暗号鍵K3jの配布を受けた1次ユーザ13は、この第3暗号鍵K3jを用いて平文2次著作権データD2jを暗号化し、

$ED2j = E(K3j, D2j)$

1次ユーザ13の記憶装置21内には暗号化データED2jが保存される。この暗号化データED2jを利用する場合には第3暗号鍵K3jを用いて復号化および暗号化が行われる。

【0045】1次ユーザ13により加工された平文2次著作権データD2jには、情報提供者が有する加工される前の平文1次著作権データD1iの1次著作権に加えて、データ加工についての2次著作権が存在する。この2次著作権を行使するために1次ユーザ13は鍵管理センタ12に3次暗号鍵K3jとともに、データのタイトル名、使用しているアプリケーション・プログラム名、内容概要、1次著作権者名を送り、鍵管理センタ12は3次暗号鍵K3jとともに保管し、管理する。

【0046】一方、1次ユーザ13は暗号化された2次著作権データED2jを外部記憶媒体18への複写あるいはネットワークシステム14を介して転送することにより2次ユーザ24へ供給する。

【0047】供給された暗号2次著作権データED2jの利用を希望する2次ユーザ24は、鍵管理センタ12に3次暗号鍵K3jの配布を要求する。この3次暗号鍵K3jによる平文2次著作権データD2jの利用は平文2次著作権データD2jの一般的な利用及びユーザ装置内への保存に限定され、平文2次著作権データD2jあるいは暗号化2次著作権データED2jの外部記憶媒体18への複写あるいはネットワークシステム14を利用することによる3次ユーザへの転送及び平文2次著作権データD2jの加工を行うことはできない。

【0048】前に述べたように、本発明において扱う著作権データはプログラムとデータが一体化した「オブジェクト」を対象としており、このオブジェクトはコンピュータプログラミングあるいは各種処理において部品の取り扱いをすることができる。図5および図2により、オブジェクトである複数の著作権データを利用して新しい著作権データを作る場合について説明する。図5において、31、32、33は各々オブジェクトとして構成された著作権データD11、D12、D13であり、これらの著作権データD11、D12、D13を利用して新しい著作権データD2j30が作成される。著作権データD11、D12、D13の利用形態としては、34に示された著作権データD11のようにその全部を利用する、35に示され

た著作権データD12のようにその一部を利用するあるいは36に示された著作権データD13のように修正して利用する、の3形態がある。

【0049】著作権データの加工は、オブジェクト単位で著作権データをリンクして引用して重ね合わせ/組み合わせを行うことにより加工処理が行われ、このような重ね合わせおよび組み合わせは自由に行うことができる。また、このように重ね合わせ/組み合わせが行われた著作権データ37にさらに他の事項を付け加えることもできる。このようにして新規に作成された著作権データD2jはオブジェクトの集合体として構成されている。

【0050】このようにして作成された平文2次著作権データD2jには1次著作権データD1iの著作権の他に新たに加工を行った1次ユーザ13の2次著作権が発生する。この2次著作権を行使するためには平文2次著作権データの暗号化が必要であり、そのために1次ユーザ13は3次暗号鍵K3jを用意し、平文著作権データD2jを3次暗号鍵K3jを用いて暗号化し、

$ED2j = E(K3j, D2j)$

外部記憶媒体18への複写あるいはネットワークシステム14を介して転送することにより2次ユーザ19へ供給する。また、3次ユーザが3次暗号鍵K3jを容易に入手することができるように、鍵管理センタ12に第3暗号鍵K3jを登録する。この第3暗号鍵K3jの登録により、1次ユーザ13の2次著作権が鍵管理センタ12に記録される。

【0051】このとき1次ユーザ13から鍵管理センタ12に送られるのは、作成した複数の2次著作権データの数に対応した複数個の第3暗号鍵K3jの他に、第3暗号鍵K3jの数、2次暗号鍵K2i、使用した1次著作権データ、著作権管理プログラムがリンクしている他の著作権データの情報、使用した著作権データへのアクセスパス、使用した著作権データが使用しているアプリケーションプログラムおよび著作物説明文章等である。

【0052】供給された暗号2次著作権データD2jの利用を希望する2次ユーザ19は、鍵管理センタ12に第3暗号鍵K3jの配布を要求する。第3暗号鍵K3jの配布要求を受けた鍵管理センタ12は、第3暗号鍵K3jをネットワークシステム14を経由して2次ユーザ19に配布する。第3暗号鍵K3jを受け取った2次ユーザ19は、第3暗号鍵K3jを用いて暗号2次著作権データED2jを復号・平文化し、利用する。

【0053】著作権管理プログラムPCは、第3暗号鍵K3jを受け取ると、それぞれの著作権データD2jに著作権ラベルLC2jを付けて2次利用者が利用可能な状態にする。この時、新規作成の著作権データとリンクされていたオブジェクトである著作権データとのリンクが解除される。解除された時点で、リンク関係だけであった利用著作権データの实体が、新規著作権データED2jに埋め込まれ、ED2jファイルだけで著作物の流通が可能と

10

20

30

40

50

なる。この場合も、暗号著作権データED2jを再度利用する場合には第3暗号鍵K3jを用いて復号化および暗号化が行われる。

【0054】鍵管理センターは、第3暗号鍵K3jを要求元に返送するとともに、著作権ラベルLC1及びLC2をもとに課金処理を行う。著作権データ所有者は、鍵管理センターに申請することにより自分の著作権データのアクセスパスを変更することができる。著作権データの所有者は、第3暗号鍵K3jで自分の著作権データを加工（修正）することも可能であり、さらに、別の鍵で登録

することも可能である。

【図面の簡単な説明】

【図1】本発明が対象とするデータ著作権管理システムの構成図。

【図2】本発明のデータ著作権処理システム実施例の概要構成図。

【図3】本発明において著作権管理プログラムPCが行う1次利用の制限を説明する概念図。

【図4】本発明において著作権管理プログラムPCが行うデータ加工利用の制限を説明する概念図。

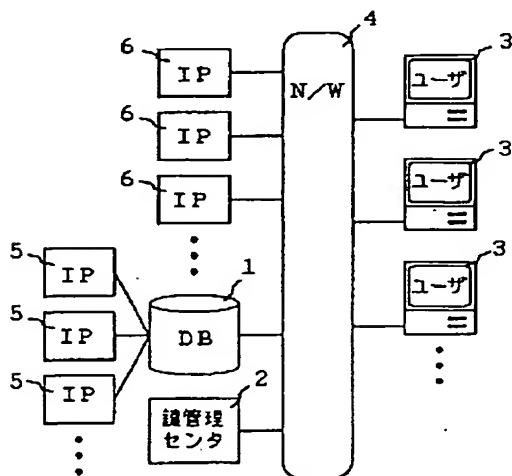
【図5】オブジェクトである複数の著作権データを利用しての新しい著作権データ作成の説明図。

【符号の説明】

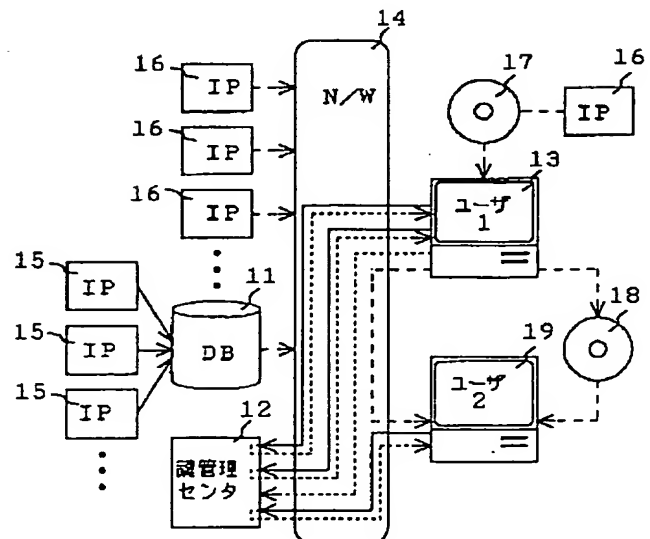
- 1, 11 データベース
- 2, 12 鍵管理センタ
- 3 ユーザ

- 4 ネットワークシステム
- 5, 6, 15, 16 情報提供者
- 11 データベース
- 12 鍵管理センタ
- 13 1次ユーザ
- 14 ネットワークシステム
- 17 情報記録媒体
- 18 外部記憶媒体
- 19, 24 2次ユーザ
- 20 1次ユーザの装置
- 21 記憶装置
- 22 表示装置
- 23 印刷装置
- 24 2次ユーザ
- 30 新しい著作権データ
- 31, 32, 33 著作権データ
- D 一般データ
- D1 1次著作権データ
- D1i 平文1次著作権データ
- 20 D1i' 加工用平文1次著作権データ
- D2j 平文2次著作権データ
- ED1i 暗号1次著作権データ
- ED2j 暗号化データ
- K1i 第1暗号鍵
- K3j 第3暗号鍵
- PC 著作権管理プログラム

【図1】

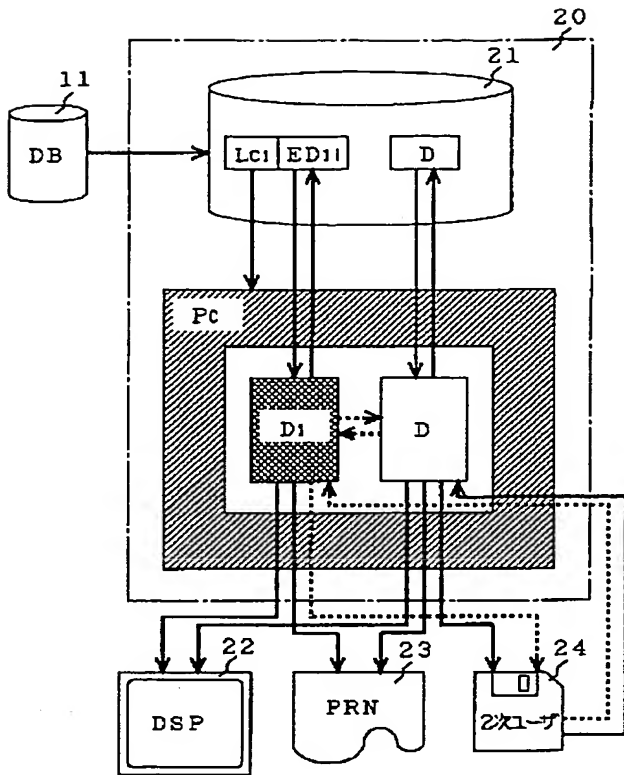


【図2】

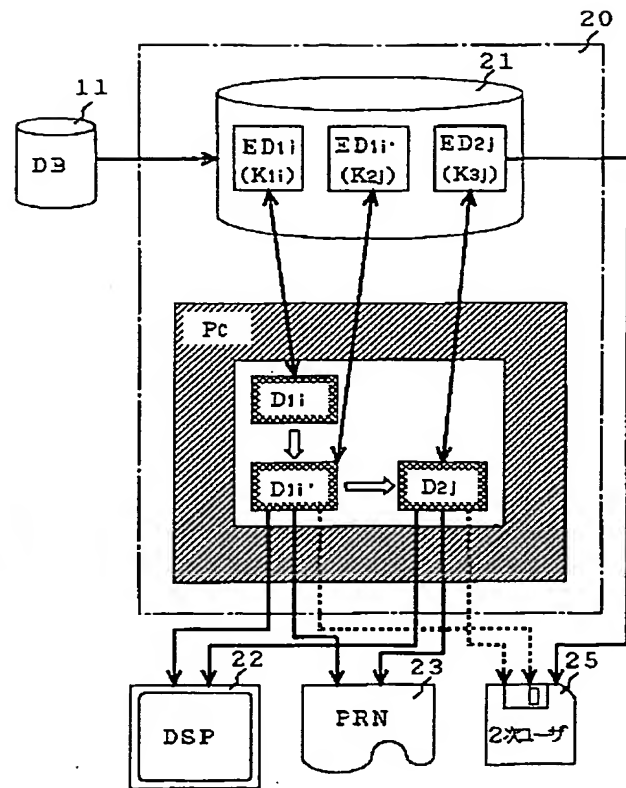




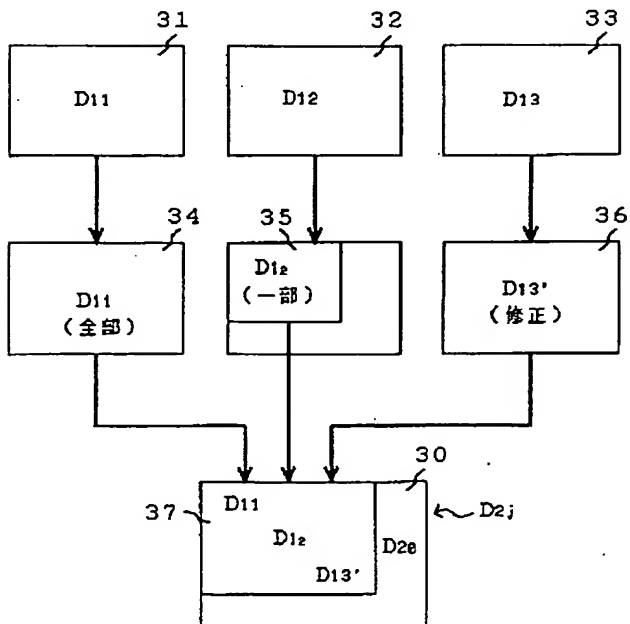
【図 3】



【図 4】



【図 5】



## フロントページの続き

| (51) Int. Cl. <sup>6</sup> | 識別記号  | 庁内整理番号 | F I     | 技術表示箇所 |
|----------------------------|-------|--------|---------|--------|
| H 0 4 L                    | 9/14  |        | H 0 4 N | 7/167  |
| H 0 4 N                    | 7/167 |        |         |        |